REMARKS/ARGUMENTS

Claims 1-20 are pending. As an initial matter, Applicant notes Examiner's statement on page 2 of the present office action that:

> "Applicant's arguments filed on 11/28/03 have been fully considered but they are not persuasive because of the following reasons.
>
> Applicant argued Vancellete does not meet the limitations as stated in independent claims 1, 15, and 18. This is not found persuasive due to the new grounds of rejection shown below.
>
> The examiner asserts that the prior art does teach or suggest the subject matter broadly recited in independent Claims 1, 15, and 18. Dependent claims 2-14, 16-17 and 19 and 20 are also rejected at least by virtue of their dependency on independent claims and by other reasons set forth in this office action (Paper No. 7). Accordingly, rejections for claims 1-20 are respectfully maintained."

In view of the above, it is unclear whether the Examiner is maintaining rejection of claims 1-20 under 35 USC 102(e) as being anticipated by Vacellete, or has withdrawn the '102(e) rejection and is merely alleging unpatentability of the present claims in view of the newly cited prior art rejections. Applicant submits that the rejection of claims 1-20 under 35 USC 102(e) as anticipated by Vancellete was successfully traversed in its response to the previous office action for the reasons discussed in said previous response. Acknowledgement of Examiner's withdrawal of this 35 USC 102(e) rejection is requested.

Rejection of claim 1 under 35 USC 103(a) as being unpatentable over Nagel et al (U.S. Patent 5,592,549) in view of Gammie et al (U.S. Patent 5,237,610)

This 35 USC 103(a) rejection is traversed, as Examiner has failed to establish a prima facie case of obviousness. More particularly, as discussed below, a) a detailed review of the references reveals that the teachings attributed to these references by the Examiner are in fact not supported by

their disclosures and hence, the claim limitations recited in present claim 1 are not rendered obvious by the combination of Nagel et al. and Gammie et al.; and b) no motivation exists for Examiner's proposed combination of the teachings of Nagel et al. in view of Gammie et al., absent impermissible hindsight gleaned from Applicant's own disclosure.

Independent claim 1 recites:

> A method for managing access to a scrambled event from a service provider, said method comprising:
>
> (a) receiving in a device associated with the user an electronic list of events, at least one event having an encrypted message associated therewith;
>
> (b) receiving in said device, in response to user selection of said event, said encrypted message;
>
> (c) decrypting said encrypted message to obtain a descrambling key;
>
> (d) receiving said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event; and
>
> (e) descrambling said selected event using said descrambling key.

In contrast, the Nagel et al. reference discloses a system for retrieving information from a secure electronic information source wherein a user at a workstation (10) selects an item of information (IP) for retrieval from a CD-ROM reader (12). The CD-ROM may contain both encrypted IP as well as IP that is clear text (i.e. not encrypted). The selected IP is part of a list of possible IP items on the CD-ROM selectable by the user. In response to user selection at the workstation of a particular IP item from the list, a decryption controller (14) determines whether the IP requested for retrieval is encrypted IP, and if so, the decryption controller retrieves the encrypted IP item or IP "message" from the CD-ROM; decrypts the IP "message" using a decryption key stored in the decryption controller to obtain a decrypted IP "message"; adds select information (i.e. clear text copyright or brand code information) to the decrypted IP "message"; and transmits to the workstation the decrypted "message" (i.e. the decrypted IP item) originally selected by the user. Thus, the system of Nagel merely decrypts a message (i.e. decrypts the IP item selected to be retrieved from the list

presented to the user) and sends the decrypted message or IP item to the user. Nagel fails to disclose or suggest portions of each of the limitations recited in steps (a) - (e) of method claim 1.

More particularly, claim 1 requires in step (a) "receiving in a device associated with the user an electronic list of events, at least one event having an encrypted message associated therewith." The Examiner purports that the "encrypted message" recited in claim 1 is represented in Nagel et al. by the encrypted IP item stored in CD-ROM (see office action, page 4, lines 4-7). Assuming arguendo the Examiner's logic, then Nagel et al. clearly fails to teach the method step (c) of "decrypting said encrypted message to obtain a descrambling key" because the "encrypted message" of Nagel is the encrypted IP item, which is the desired data to be obtained by the user (in decrypted form). The Examiner acknowledges this deficiency of Nagel et al on page 4, lines 11-12 of the present office action.

In addition, however, it necessarily follows that Nagel et al. also fails to suggest the limitation in step (d) of "receiving said selected event from the service provider, said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event". This omission in the primary reference is evidenced by the fact that Nagel et al. teaches scrambling or encryption of only the selected "IP item", which item the Examiner already associated with the claim limitation "encrypted message" referred to in steps (b) and (c) above. Accordingly, the IP item of Nagel et al. cannot be both the "encrypted message" and also the "scrambled selected event" limitations recited in method claim 1. Moreover, it follows that Nagel et al. also cannot meet the additional limitation of the scrambled selected event "scrambled using said descrambling key", as Nagel does not even hint at a descrambling key obtained in this manner. Finally, Nagel et al. cannot meet the limitation of step (e) of "descrambling said selected event using said descrambling key" when such descrambling key was neither disclosed nor contemplated in the manner recited in claim 1 as a whole.

Accordingly, Applicant submits that a detailed reading of Nagel et al reveals that the primary reference fails to disclose or suggest significant aspects of steps (a), (c), (d) and (e) of independent method claim 1. The Gammie et al. reference fails to cure the above noted deficiencies of the primary reference. Such a combination is merely a piece-meal selection of individual elements from Nagel et al. and Gammie et al., which combination is not supported by the teachings of any of these references. Therefore, present claim 1 is not obvious in view of the proposed combination of Nagel

et al. in view of Gammie et al. and should be allowed, as should all of claims 2-14 depending therefrom. Withdrawal of this 35 USC 103(a) rejection is requested.

The above notwithstanding, Applicant submits that nowhere in either the references themselves, or in the teachings of the prior art, is there any motivation or desire to somehow combine these two references in an attempt to reach the present invention. Moreover, the primary reference not only fails to provide a motivation or suggestion for its modification, but in fact teaches away from such proposed modification and combination with the secondary reference.

On page 3 of the present office action, the examiner states that "the Nagel system suggests receiving in a device an electronic list of events, at least one event having an encrypted message associated therein." The Examiner further states that the list is associated with an encrypted message since the information on the CD-ROM is encrypted, and that the encrypted message is received in response to user selection of said event. The Examiner admits that Nagel "does not expressly disclose decrypting the encrypted message to obtain a descrambling key." However, the Examiner attempts to bolster the primary reference by asserting that Gammie discloses a system for descrambling encoded transmissions wherein the program is scrambled using a key and where the key itself is twice encrypted and multiplexed with the scrambled program signal. The scrambled signal and encrypted keys are then demultiplexed, and the keys are decrypted to obtain a descrambled key which is then used to descramble a given scrambled signal. The Examiner concludes that "at the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the twice-descrambling method of Gammie in the system disclosed by Nagel. One of ordinary skill in the art would have been motivated to do this because keys distributed to an authorized decoder cannot be read out and transferred to other decoders."

In response, Applicant submits that no motivation exists for Examiner's purported combination, absent impermissible hindsight, and that the primary reference in fact teaches away from such combination. More particularly, Examiner's attention is directed to Column 8, lines 22-23 of Nagel et al., which recites "All keys utilized by the system are created and maintained in the decryption controller" (emphasis added). Nevertheless, the Examiner improperly attempts to combine Gammie with Nagel et al. in order to introduce the teaching of an encrypted key that is eventually decrypted and ultimately used to decrypt a selected event in an attempt to arrive at Applicant's claimed invention. However, Gammie et al. teaches that the keys used by the system, and

particularly, the twice encrypted keys used to decrypt scrambled programs, are not to be created and maintained in the decryption controller, but instead and by design are generated remote from the decryption controller and then sent to the decryption controller for use. Thus, Examiner's purported combination would modify the primary reference of Nagel et al. to utilize a key that was not created in the controller to descramble an IP item. Such modification is contrary to the teachings of Nagel et al. and entirely without motivation or suggestion in the references themselves, absent impermissible hindsight gleaned from Applicant's own specification.

M.P.E.P. § 2142 states:

> *To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See MPEP § 2143 - § 2143.03 for decisions pertinent to each of these criteria.*

Because there would have been no motivation to combine Nagel et al. which teaches creation and utilization of keys within its decryption controller, with the teachings of Gammie et al., which requires an encrypted key be remotely created and later sent to the controller to be twice decrypted and then used to decrypt an encrypted IP item, a prima facie case of obviousness has not been established. Reconsideration and withdrawal of this 35 USC 103(a) rejection is respectfully requested.

Rejection of claims 15, 18 under 35 USC 103(a) as being unpatentable over Nagel et al (U.S. Patent 5,592,549) in view of Gammie et al (U.S. Patent 5,237,610) and Pinder et al (U.S. Patent 5,742,677)

Independent Claims 15 and 18 stand rejected under 35 USC 103(a) as being unpatentable over Nagel et al in view of Gammie et al and further in view of Pinder et al. The arguments discussed hereinabove with regard to claim 1 apply as well to these claims. Moreover, Pinder does nothing to overcome the deficiencies associated with the Nagel et al and Gammie et al. references discussed above. Still further, present claims 15 and 18 recite further additional features, including the use of a "symmetric key" for scrambling/descrambling, and of a "first public key" and "second private key" for performing the authentication prior to descrambling of the actual event or program received at the device. For at least these reasons, present claims 15 and 18 are patentable in a '103 sense and should be allowed, as should all claims depending therefrom. Reconsideration and withdrawal of this 35 USC 103(a) rejection is respectfully requested.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, claims 1-20 of this application stand in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 919-4428, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully Submitted

Date: May 12, 2004

Edward J. Howard
Registration No. 42,670

DUANE MORRIS LLP
100 College Road West, Suite 100
Princeton, NJ 08540
Tel: (609) 919-4428
Fax: (609) 919-4401

PTN\45771.1